

# **Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review**

*CSWG Standards Review Report*

***ZigBee Smart Energy Profile Specification 1.0***

***Document 075356r15, 2008***

***Smart Energy Profile Specification Version 1.0***

**July 18, 2011**



# Security Assessment of ZigBee Smart Energy Profile Specification Document 075356r15

## 1. Introduction

### 1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different “layers” in the communications “stack” or “profile,” one example of such a profile is the GridWise Architecture Council (GWAC) Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the “transport” layers for getting messages from one location to another. Still others cover the “application” layers, the semantic structures of the information as it is transmitted between software applications. There are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into “bits and bytes” by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself. Conversely, cybersecurity vulnerabilities identified within a standard may be compensated for by adjacent standards that represent any end-to-end system that employs a defense in depth strategy across heterogeneous physical and transport layers. The requirements must include how and where a standard is used, and must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance. Fourthly, some standards do not mandate their provisions using “shall” statements, but rather use statements such as “should,” “may,” or “could.” Some standards also define their provisions as being “normative” or “informative.” Normative provisions often are expressed with “shall” statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the “shall,” “should,” “may,” and/or “could” statements, “normative,” or “informative” language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or “profile” of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity, as applied to the information exchange standards, should be described as profiles of technologies and procedures which can include both “power system” methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then transport layer security (TLS) should most likely also be used.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

## **1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements**

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

## **1.3 Standardization Cycles of Information Exchange Standards**

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

## **1.4 References and Terminology**

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

The terms “approved”, “acceptable”, and “deprecated” are defined as the following<sup>1</sup>:

- Approved is used to mean that an algorithm is specified in a FIPS or NIST Recommendation (published as a NIST Special Publication).
- Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.

---

<sup>1</sup> The definitions are obtained from NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

- Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

References to “government-approved cryptography” refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees<sup>2</sup>:

- Requirements are expressed by “...shall...,” which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall equals is required to*).
- Recommendations are expressed by “...should...,” which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should equals is recommended that*).
- Permitted or allowed items are expressed by “...may...,” which is used to indicate a course of action permissible within the limits of the standard (*may equals is permitted to*).
- Ability to carry out an action is expressed by “...can ...,” which is used for statements of possibility and capability, whether material, physical, or causal (*can equals is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. “All traffic in this lane must turn right at the next intersection.”)

## 2. ZigBee Smart Energy Profile Specification, Document 075356r15 (SEP 1.0)

### 2.1 Description of Document

According to the ZigBee Smart Energy Profile Specification, known also as SEP 1.0, “*This profile defines device descriptions and standard practices for Demand Response and Load Management “Smart Energy” applications needed in a Smart Energy based residential or light commercial environment. Installation scenarios range from a single home to an entire apartment complex. The key application domains included in this initial version are metering, pricing and demand response and load control applications. Other applications will be added in future versions.*”

The next revision to this document is ZigBee Smart Energy Profile Specification, Document 075356r16ZB (SEP 1.1). Both SEP 1.0 and 1.1 are planned to be eventually replaced by SEP 2.0.

Security issues are primarily covered in:

- Section 5.3.3 Security Parameters
- Section 5.4 Smart Energy Profile Security
- Annex C Key Establishment Cluster

### 2.2 Assumptions Related to Cybersecurity

All seven (7) layers of the Open Systems Interconnection (OSI) model appear to be discussed throughout the document, but at a high-level. *It is assumed that* there is not a one-to-one correlation with the

---

<sup>2</sup> The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after “which”) comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

documented approach with each layer, but the solution architectures provided address the transport service and upper layers. This may be because the documents were developed prior to the review guide.

The document refers primarily to technologies, with solution architectures identified, by providing high-level standard interfaces and device definitions that will allow interoperability among devices produced by various manufacturers of electrical equipment, meters, and Smart Energy enabling products.

The policies and procedures for cybersecurity were not addressed directly in the document. This information may be covered in the seven ZigBee documents listed in Section 2.3.6.1, but the CSWG reviewers did not include those documents as part of this review.

The ZigBee SEP 1.0 and 1.1 specifications, Section 5.1, imply applicability for Customer Home Area Network (HAN), Utility Home Area Network and Utility Neighborhood Area Network (NAN). However, the remaining sections of these documents address security for Customer Home Area Networks only. Therefore, this review by the CSWG has outlined concerns only for the Customer Home Area Network. A more detailed evaluation of the security requirements for the Utility Home Area Network and Utility NAN is required to provide a complete security analysis of the standard. Specifically, devices which can directly interact with utility back office systems (as is the case of Utility NANs) would require additional in depth evaluation.

A document developed by Robert Cragie<sup>3</sup> provides additional insight into the security implications of SEP 1.0 and 1.1. This analysis is outside of the scope of the CSWG Standards subgroup.

## **2.3 Assessment of Cybersecurity Content**

### **2.3.1 Does the standard address cybersecurity? If not, should it?**

The document addresses cybersecurity in Section 5.4, Annex C, Annex D, and Annex F.

However, the standards referenced throughout the document do not directly address cybersecurity or follow guidelines specified by the Open Standard Interconnect (OSI) layers and the GWAC Stack. At a minimum, the document should cover OSI layers 1 through 4. Attacks from outside the network are addressed at a high level, but those from the inside going out are not addressed. For example, security requirements are not included in SEP 1.0 and 1.1 that cover compromised devices from within the network, or addition of a NAN device on the system for interacting and obtaining information to that could be used in other security attack attempts outside the network.

### **2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?**

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in

Table 1.


---

<sup>3</sup> Cragie, Robert, "SEP 1.x Cybersecurity Review", June 2011, available at: <http://collaborate.nist.gov/wiki-sgrid/bin/view/SmartGrid/CSTGStandards>

**Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements**

Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
<p>1.2 ZigBee Definitions</p> <p><b>ZigBee coordinator:</b> An IEEE 802.15.4-2003 PAN coordinator.</p> <p><b>ZigBee end device:</b> an IEEE 802.15.4-2003 RFD or FFD participating in a ZigBee network, which is neither the ZigBee coordinator nor a ZigBee router.</p> <p><b>ZigBee router:</b> an IEEE 802.15.4-2003 FFD participating in a ZigBee network, which is <b>not</b> the <b>ZigBee coordinator</b> but may act as an IEEE 802.15.4-2003 coordinator within its personal operating space, that is capable of routing messages between devices and supporting associations.</p>	<p>SG.AC-2: Remote Access Policy and Procedures</p> <p>SG.AC-5: Information Flow Enforcement</p> <p>SG.AC-7: Least Privilege</p>	<p>NISTIR requirements for cybersecurity are not completely met; the specification of these roles does not guarantee fulfillment of the NISTIR requirements.</p>
<p>2.1.1 Zigbee Alliance Documents Reference to 075297r04</p>	<p>SG.IA-5: Device Identification and Authentication</p> <p>SG.AC-15: Remote Access</p>	<p>The Inter-PAN feature allows unauthenticated devices to communicate into a networked device without any security or authentication.</p>
<p>5.1 A ZigBee Smart Energy Network</p>	<p>SG.AC-2: Remote Access Policy and Procedures</p> <p>SG.AC-5: Information Flow Enforcement</p>	<p>NISTIR requirements for cybersecurity are not completely met.</p> <p>Section 5.1 allows for 3 different topologies with differing security requirements:</p> <ol style="list-style-type: none"> <li>1. A Utility Private HAN;</li> <li>2. A Utility Private NAN; and</li> <li>3. A Customer Private HAN.</li> </ol> <p>Since the Utility Private NAN touches the utility back office network, the security concerns around policy and access should have been different from the HAN. In general, only the Customer Private HAN security is dealt with in the specification.</p>

<sup>4</sup> The references may be just the section numbers or could include the title of the section, depending upon what fits easily.

Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.2 ZigBee Stack Profile	SG.AC-2: Remote Access Policy and Procedures  SG.AC-5: Information Flow Enforcement	NISTIR requirements for cybersecurity are not completely met.  Section 5.2.1 details two configurations for the Trust Center: 1. For the HAN, and 2. For the NAN.  Only the location of the Trust Center is outlined and there is no mention of the different security domains and associated security policies.
5.3 Startup Attribute Set (SAS)	SG.AC-2: Remote Access Policy and Procedures	NISTIR requirements for cybersecurity are not completely met.  Section 5.3 details the required startup attribute set parameters and their settings, but there is no mention about security for these attributes (both pre-installation and post-installation). Since the Network Key, Link Keys, and Trust Center address are part of these attributes, some set of security policies should pertain to access control.
5.4 Smart Energy Profile Security  Annex C Key Establishment Center  Annex F Joining Procedure Using Pre-Configured Trust Center Link Keys	SC.AC-4: Access Enforcement	Section 5.4.1 fulfills this requirement, however Section 5.4.2, Re-join, does not enforce appropriate access control.
5.4.1 Joining Smart Energy Network  5.4.8.2 Managing and Initiating Registration Processes	 SG. pubring.pkr SC-7: Boundary Protection	
5.4.1 Joining with Preinstalled Link Keys	SG.AC-1: Access Control Policy and Procedures	
5.4.1 Joining with Preinstalled Trust Center Link Keys  5.4.2 Re-Joining a Secured Network  5.4.7 Key Establishment Related Security Policies	SG.IA.5: Device Identification and Authentication	Section 5.4.1 fulfills this requirement; however, 5.4. Re-join, does not enforce appropriate access control.

Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.4.1 Joining with Preinstalled Trust Center Link Keys  5.4.2 Rejoining a Secure Network  Annex F Joining Procedure Using Pre-Configured Trust Center Link Keys	SC.AC-16: Wireless Access Restrictions	This requirement is met by the use of the network key.
5.4.1 Joining with Preinstalled Trust Center Link Keys  5.4.2 Rejoining a Secure Network  Annex F Joining Procedure Using Pre-Configured Trust Center Link Keys	SC.AC-17: Access Control for Portable and Mobile Devices	Section 5.4.1 fulfills this requirement, however 5.4.2, Re-join, does not enforce appropriate access control.
5.4.2.2 Trust Center Operation	SG.CA1: Security Assessment and Authorization Policy and Procedures	Assessing the risk of malicious attacks against the Smart Grid's critical infrastructures will require modifications to existing management methodologies. Existing risk assessment methodologies consider physical security and cybersecurity separately.  As such, the Smart Energy Profile Specification does not demonstrate an approach to mitigate attacks that involve defeating both physical protection and cyber protection elements (e.g., breaches to solutions architectures deployed on the smart grid). This document does not adequately present a risk assessment methodology (confidentiality, Integrity, and availability impact levels) that accounts for both physical and cybersecurity related to solutions architectures deployed on the Smart Grid.
5.4.4 Updating the Network Key	SG.SC-11: Cryptographic Key Establishment and Management	It is unclear how broadcasting a new Network Key to all members of a PAN helps in Network Key management.
5.4.4 Updating the Network Key  5.4.5 Updating the Link Key	SG.SC-11: Cryptographic Key Establishment and Management	While sections 5.4.4 and 5.4.5 refer to Trust Center policies around Network and Link Key management, the policies are not discussed in the referenced documentation. There appears to be no uniform policy around key management aside from the general best practice that is should be done.
5.4.6 Cluster Usage of Security Keys	SG.SC12: Use of Validated Cryptography	
5.4.7 Key Establishment Related Security Policies  5.4.8.2 Managing and Initiating Registration Processes	SG.IA.3 Authenticator Management	This applies only to devices and not to users. The standard mandates periodically changing network and link keys as specified in section 5.4.4.



Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.4.7 Key Establishment  Annex C.4.1 Network Security for Smart Energy Networks	SG.SC-11 Cryptographic Key Establishment and Management	
5.4.7.3 Key Establishment Related Security Policies During Joining  5.4.8.1 Security Best Practices Out of Band Pre-Configured Link Key Processes  Annex F Joining Procedure Using Pre-Configured Trust Center Link Keys	SG.AC-8: Unsuccessful Login Attempts  SG.AC-16: Wireless Access Restrictions  SG.IA-5: Device Identification and Authentication	Devices are admitted to the HAN without authentication. Devices employ an Install Code, which can be as short as 48 bits with no provision for preventing repeated attempts to guess the value. If this value is guessed, the device is admitted to the HAN and provided the Network Key, all before any device authentication is performed.
5.4.7.4 Key Establishment Related Security Policies After Joining	SG.AC-2: Remote Access Policy and Procedures  SG.AC-3: Account Management  SG.AC-4: Access Enforcement	No certificate revocation feature provided.
5.4.8.2 Managing and Initiating Registration Processes	SG.IA.2: Identifier Management	This applies only to devices and not to users.
5.5 Commissioning	SG.AC-2: Remote Access Policy and Procedures  SG.AC-5: Information Flow Enforcement	NISTIR requirements for cybersecurity are not completely met.  Commissioning, particularly for NAN devices which are utility assets interconnected to the utility back office, should have a security considerations section and include a discussion on security policies and access procedures.
Annex D Smart Energy Cluster Descriptions	SG.SI-9 Error Handling	
5.4.6 Cluster Usage of Security Keys  Annex F Joining Procedure Using Pre-Configured Trust Center Link Keys	SG.SC-11: Cryptographic Key Establishment and Management	Table 5.10 lists commands and expected security key usage for each command. It is possible for a man in the middle attack to occur using the Key Establishment cluster with an unauthenticated device holding the Network Key.

Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
Annex B Inter-Pan Transmission Mechanism	SG.AC-15: Remote Access  SG.IA-5: Device Identification and Authentication	NISTIR requirements for cybersecurity are not completely met.  Inter-PAN feature allows unauthenticated devices to communicate into a networked device without authentication. Any device can communicate with any other device. While none of the clusters use Inter-PAN, its presence in the standard allows implementations to be exposed to additional vulnerabilities. It is suggested that Inter-PAN be removed from SEP 1.0 and 1.1.
Annex C Key Establishment Cluster	SG.AC-8: Unsuccessful Login Attempts  SG.AC-16: Wireless Access Restrictions  SG.IA-5: Device Identification and Authentication	NISTIR requirements for cybersecurity are not completely met.  Devices are admitted to the HAN without authentication. The Key Establishment Cluster, which provides authentication, is only sent after the device has been given the Network Key for the HAN. Key Establishment should occur before admission to the network.
2.1.2 External Reference Documents (B11, B12, B13, B14)  Annex C Key Establishment Cluster  Annex C.2.3 Key Establishment  Annex C.4.2.2.5 Block-Cipher  Annex C.4.2.2.7 Keyed Hash Function for Message Authentication	SG.SC-12 Use of Validated Cryptography	SEP cryptographic function building blocks are specified by the ZigBee specification. The ZigBee specification contains a general recommendation that the pseudo random number generator (PRNG) be FIPS-140 compliant. This should be a mandatory requirement.
Annex C.2.3 Key Establishment	SG.SC-9 Communication Confidentiality	
Annex C.2.3 Key Establishment  Annex C.4.2.2.7 Keyed Hash Function for Message Authentication	SG.SC-8 Communication Integrity	
Annex C.2.5 Public Key Establishment  Annex C.4.2 Certificate-Based Key Establishment	SG.SC-15 Public Key Infrastructure Certificates	
Annex C.2.5 Public Key Establishment  Annex C.4.2 Certificate-Based Key Establishment	SG.SC-20 Message Authenticity	

Reference in Standard <sup>4</sup>	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
Annex C.2.6.2 Generate Key Bitstream	SG.SC-11: Cryptographic Key Establishment and Management	
Annex C.2.6.2 Generate Key Bitstream	SG.SC-11: Cryptographic Key Establishment and Management	Key length used in ECMQV is only 80 bits, which is too short for the lifetime for the devices it is installed in. 80 bit key lengths will be allowed in devices only until 2013, as per NIST SP 800-131A.
Annex C.4.2 Certificate-Based Key Establishment	SG.SC-15: Public Key Infrastructure Certificates	
Annex D Smart Energy Cluster Descriptions	SG.AC-2 – Remote Access Policy and Procedures SG.AC-5 – Information Flow Enforcement	NISTIR requirements for cybersecurity are not completely met.  Annex D does not include a section discussing security considerations. Since SEP 1.0 and 1.1 allows devices to join without authentication, the confidentiality of the Smart Energy Clusters should be included, as the authentication command must occur after Key establishment and authentication.
Annex D.2.4.2.3 Response to Price Events and Load Control Events	SG.SC-6: Resource Priority	Only reference to resource priorities in standard is for demand response events, where they will have higher priority than price driven events.
Annex D.3.2.2.3.1 Status Attribute	SG.SC-18: System Connections	Tamper detection is provided for, but not mandated. Tamper Detect and other damaged bit indicators can be set by the metering device, but do not prevent tampering/damage.

### 2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

- The Trust Center is identified as having a significant role in the security of the SEP 1.0 and 1.1 standard, but no requirements exist to make the Trust Center trustworthy. This standard suggests use of the meter as the Trust Center. However, the CSWG review of metering standards indicates a gap in cybersecurity for meters that would need to be filled before they could be used for that purpose.
- Certificate revocation is not supported (see 073536r15, Section 5.4.7.4)
- Devices are provided access to the Home Area Network without authentication and are supplied the HAN specific network key before authentication.
- The ECQV is an implicit certificate. Implicit certificate schemes are not assessed by NIST; rather NIST examines the underlying cryptographic suites (primitives). It is insufficient to say "it uses ECQV" – it is also necessary to include how those public keys are applied. SEP 1.0 specifies using NIST approved ECMQV and ECDSA as the cryptographic primitives for calculating the public key. If the protocol uses other variants it is important to verify, using the NISTIR 7628, Table 4.2, if they are NIST approved. For example, the Elliptic-Curve Pintsov-Vanstone Signatures (ECPVS) scheme) is not a NIST approved cryptographic primitive.
- ECMQV employs key strengths of 80 bits which can be carried in one message with the purpose of making it usable in small devices that cannot handle the breaking up of larger certificates into multiple messages. This makes the certificate too short for more security sensitive HAN devices. As stated in NIST SP800-131A, Section 1.2.1, "*The appropriate security strength to be used depends on the sensitivity of the data being protected, and needs to be determined by the owner*

*of that data (e.g., a person or an organization). For the Federal government, a minimum security strength of 80 bits is recommended in 2010; a minimum security strength of 112 bits is strongly recommended beginning in 2011 (see [SP 800-57]). However, with the acceptance of a certain amount of risk, the minimum of 80 bits of security strength may be used until the end of 2013. Based on the latest understanding of the state of the art for breaking the cryptographic algorithms, given particular key lengths, the transition to the 112-bit security strength **shall** be accomplished by 2014, except where specifically indicated."*

- The AES-128-MMO hash algorithm is not a NIST–approved algorithm.
- There is no stated key management policy for the Network Key or Link Key within the Trust Center.
- The Inter-PAN feature does not require device authentication, data encryption or integrity checking, and allows any device to interact with any other device. Although it is not currently used in any of the clusters or included in certification testing, it poses a security risk by remaining part of SEP 1.0 and 1.1 standard.
- MAC layer security is disabled because the use of the updated MAC security causes interoperability problems.
- The Network Key, used for many security-critical operations, is provided to joining devices without any device authentication.

#### **2.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?**

ZigBee performed an outside security audit using an independent organization (Carnegie Mellon) to analyze the security as dictated by the SEP 1.0. Many of the recommendations were not addressed in the SEP 1.1. SEP 2.0 is now currently being finalized, but it is not backward compatible with SEP 1.0/1.1 (although a migration path is being developed). The CSWG has provided detailed cybersecurity recommendations for consideration in the draft SEP 2.0 specification.

#### **2.3.5 Recommendations**

- Use of a cipher suite whose cryptographic strength is less than 112 bits has been deprecated by NIST. The ECQV underlying cipher suite contains 80 bit cryptographic strength. Therefore, the CSWG cannot approve this document as being compliant with the NISTIR 7628, whose focus is to provide adequate security and interoperability. The CSWG understands the concern that some appliances are not capable of handling ciphers that are larger than one message.
- In addition to addressing the security weaknesses of the ECQV underlying cipher suite, it is recommended that the Zigbee Alliance group responsible for SEP 1.0 and 1.1 should also address the cybersecurity gaps and issues identified in each of the bullet items in section 2.3.3 of this review.
- The role of the CSWG is to review standards and make recommendations on what aspects do not meet the NISTIR 7628 requirements. However to ensure adequate overall cybersecurity of SEP 1.0 and 1.1 implementations, it is also recommended that the following tasks are undertaken by the appropriate entities:
  - Develop a risk management process to assess the use of the existing ECQV underlying cyber suites with devices that have different cybersecurity requirements;
  - Provide guidelines where this risk may or may not be acceptable;
  - Develop best practices for mitigating these risks in existing implementations; and

- Define the term “Trust Centers,” and develop the security requirements for establishing and using Trust Centers.
- It is recommended that Annex B covering the Inter-PAN capabilities be removed.

## 2.3.6 List any references to other standards and whether they are normative or informative

### 2.3.6.1 Normative and Informative

- [B1] ZigBee Document 064321r08, The ZigBee Stack Profile, ZigBee Architectural Sub-Committee of the TSC (TAG)
- [B2] ZigBee document 075123r011, ZigBee Cluster Library Specification, ZigBee Application Framework Working Group.
- [B3] ZigBee document 064309r04, Commissioning Framework
- [B4] ZigBee Document 053474r17, The ZigBee Specification, ZigBee Technical Steering Committee (TSC)
- [B5] ZigBee Document 074855r04, The ZigBee PRO Stack Profile, ZigBee Architectural Sub-Committee of the TSC (TAG)
- [B6] ZigBee Document 03084r00, ZigBee Key Establishment Proposal Certicom
- [B7] ZigBee 075297r04, Proposal for Inter-PAN Exchange of Data in ZigBee
  - 1. CCB 964
- [B8] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4 2003, IEEE Standard for Information Technology Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs). New York: IEEE Press. 2003
- [B9] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American Bankers Association. Available from <http://www.ansi.org>. <http://www.ansi.org>.
- [B10] ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography, American Bankers Association, November 20, 2001. Available from <http://www.ansi.org>. <http://www.ansi.org>.
- [B11] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007. Available from <http://csrc.nist.gov>. <http://csrc.nist.gov>.
- [B12] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004. Available from <http://csrc.nist.gov>. <http://csrc.nist.gov>.
- [B13] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001. Available from <http://csrc.nist.gov>. <http://csrc.nist.gov>.
- [B14] FIPS Pub 198, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198, US Department of Commerce/N.I.S.T., Springfield, Virginia, March 6, 2002. Available from <http://csrc.nist.gov>. <http://csrc.nist.gov>.

- [B15] Standards for Efficient Cryptography: SEC 1 (working draft) ver 1.7: Elliptic Curve Cryptography, Certicom Research, November 13, 2006. Available from <http://www.secg.org><http://www.secg.org>
- [B16] Standards for Efficient Cryptography: SEC 4 (draft) ver 1.1r1: Elliptic Curve Cryptography, Certicom Research, June 9, 2006. Available from <http://www.secg.org> :// [www.secg.org](http://www.secg.org)
- [B17] RFC 3280: Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. IETF, April 2002. Available from <http://www.ietf.org> <http://www.ietf.org>